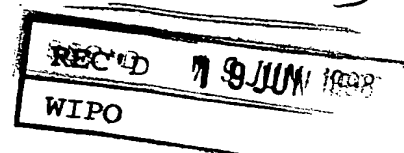


22.04.98

3

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1997年 4月24日

出 願 番 号
Application Number:

平成 9年特許願第106995号

出 願 人
Applicant (s):

松下電器産業株式会社

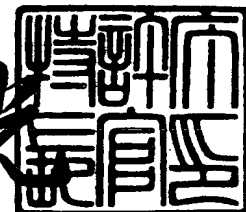
BEST AVAILABLE COPY

PRIORITY DOCUMENT

1998年 6月 5日

特 許 庁 長 官
Commissioner,
Patent Office

荒井 寿光



出証番号 出証特平10-3042512

【書類名】 特許願

【整理番号】 2054091207

【提出日】 平成 9年 4月24日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00

【発明の名称】 データ転送方法

【請求項の数】 13

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 西村 拓也

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 飯塚 裕之

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 山田 正純

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100078204

【弁理士】

【氏名又は名称】 滝本 智之

【選任した代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9702380

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ転送方法

【特許請求の範囲】

【請求項1】 バス上の任意の機器が同期データを受信する同期通信と、非同期データを受信する機器が特定される非同期通信とが混在するバスシステムにおいて、前記同期データは実データ部を含む場合があり、前記実データ部の暗号化状況を示す暗号識別情報が前記実データ部以外の前記同期データ中に含まれており、前記同期データを受信した受信装置は、前記実データ部が暗号化されていることを前記暗号識別情報が示している場合には前記同期データを送信している送信装置に対して前記非同期通信を用いて前記実データ部の復号化情報を要求し、前記要求を受けた前記送信装置は前記非同期通信を用いて前記受信装置に対して前記実データの復号化情報を暗号化して送信し、前記受信装置は前記暗号化された復号化情報から前記復号化情報を取り出し、前記復号化情報を用いて暗号化された実データ部を復号することを特徴とするデータ転送方法。

【請求項2】 同期データを受信した受信装置が実データ部が暗号化されていることを検出してから復号化情報を取得するまでの一連の手順には複数の種類が存在し、前記受信装置は復号化情報の要求に先立って送信装置が実行可能な手順の種類を前記送信装置に問い合わせ、前記受信装置は自身と前記送信装置との双方が実行可能な前記手順の中から実行する手順を選択し、前記受信装置は選択した手順に基づいて前記復号化情報を取得することを特徴とする請求項1記載のデータ転送方法。

【請求項3】 選択された手順に基づいて送信装置と受信装置との間で授受される非同期データには、実行中の前記手順の種類をあらわす手順識別子が含まれることを特徴とする請求項2記載のデータ転送方法。

【請求項4】 受信装置は、復号化情報の要求を行う前に、送信装置が正規の送信装置であることを確認することを特徴とする請求項1、2または3記載のデータ転送方法。

【請求項5】 送信装置は復号化情報の要求を受けた後、受信装置が正規の受信装置であることを確認してから実データの復号化情報を暗号化して送信するこ

とを特徴とする請求項1、2または3記載のデータ転送方法。

【請求項6】 送信装置と受信装置とが互いに、相手が正規の受信装置または正規の送信装置であることを確認してから前記受信装置が復号化情報の要求を行うことを特徴とする請求項1、2または3記載のデータ転送方法。

【請求項7】 受信装置が復号化情報を要求する前に、前記受信装置から送信装置に対して前記送信装置が共通鍵を作成するのに少なくとも必要な情報の送信と、前記送信装置から前記受信装置に対して前記受信装置が前記共通鍵を作成するのに少なくとも必要な情報の送信とが行われ、前記送信装置は前記共通鍵を用いて前記復号化情報を暗号化して送信し、前記受信装置は前記共通鍵を用いて前記復号化情報を取り出すことを特徴とする請求項1ないし6のいずれかに記載のデータ転送方法。

【請求項8】 暗号化は実データ部に対してのみ行うことを特徴とする請求項1、2または3記載のデータ転送方法。

【請求項9】 送信装置は内部に実データの信号源を有し、前記送信装置は前記信号源から出力された固定長単位の前記実データ毎に暗号化の有無を決定し、暗号化された前記実データと暗号化されていない前記実データとを互いに異なる同期通信の出力単位内に配置してバスシステムへ出力することを特徴とする請求項1、2または3記載のデータ転送方法。

【請求項10】 暗号化された実データと、暗号化されない実データとの比率を受信装置が送信装置に対して非同期通信を用いて指定し、前記送信装置は前記指定に従って暗号化の有無の比率を変更することを特徴とする請求項9記載のデータ転送方法。

【請求項11】 送信装置は内部に実データの信号源を有し、前記送信装置は前記信号源から出力された固定長単位の前記実データについて、前記固定長単位の中での暗号化を行う割合を決定し、前記実データを同期通信の出力単位内に配置してバスシステムへ出力することを特徴とする請求項1、2または3記載のデータ転送方法。

【請求項12】 受信装置は送信装置に対して、暗号化を行う割合の指定を非同期通信を用いて行い、前記送信装置は前記指定に従って暗号化する割合を変更

することを特徴とする請求項11記載のデータ転送方法。

【請求項13】 送信装置が同期データを送信する際に、少なくとも復号化情報を要求されるまでの間は前記同期データに実データ部を含めずに送信し、少なくとも前記復号化情報の要求を受け取った後に前記実データ部を含んだ前記同期データの送信を開始することを特徴とする請求項1、2または3記載のデータ転送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタルデータを送受信する機器間のデータ転送方法に関するものである。

【0002】

【従来の技術】

従来のデータ転送方式には、IEEE1394規格(IEEE:THE INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, INC)を用いたデータ転送方法がある。

(参考文献:IEEE1394 High Performance Serial Bus) IEEE1394規格におけるデータ転送には、映像信号や音声信号等の同期データの転送に適したアイソクロノス通信と、制御信号等の非同期データの転送に適したエイシンクロナス通信とがあり、両通信はIEEE1394バス上で混在することが可能である。アイソクロノス通信はいわゆる放送型の通信であり、IEEE1394バス上のある装置が出力するアイソクロノスパケットは、同バス上の全ての装置が受信することができる。これに対してエイシンクロナス通信は1対1の通信と放送型通信の両方があり、バス上のある装置が出力するエイシンクロナスパケットにはそのパケットを受信すべき装置をあらわす識別子が含まれており、その識別子が特定の装置をあらわす時にはその識別子で指定された装置が当該エイシンクロナスパケットを受信し、識別子がブロードキャストをあらわす時には同バス上の全ての装置が当該エイシンクロナスパケットを受信する。

【0003】

また、IEEE1394規格を用いてデジタル音声信号やデジタル映像信

号等を転送したり、IEEE 1394バス上につながれた機器間でデータ伝送経路の接続管理を行うための規格として、IEC (IEC:International Electronic Commission 国際電気標準会議)においてIEC 1883規格(以下、AVプロトコルと称する)が検討されている。AVプロトコルにおいては、映像音声データはアイソクロノスケット内に配置されて転送される。また、アイソクロノスケットはCIPヘッダ(CIP:Common Isochronous Packet)を含む。CIPヘッダ内には映像音声データの種別を示す識別情報や、アイソクロノスケットを送信している送信装置の装置番号等の情報が含まれている。

【0004】

図5は、AVプロトコルにて使用されるアイソクロノスケットのフォーマットをあらわす図である。アイソクロノスケットはアイソクロノスケットヘッダ900、ヘッダCRC901、アイソクロノスペイロード902、データCRC903からなる。アイソクロノスケットヘッダ900にはタグ907が含まれる。タグ907は、その値が1である時にはそのアイソクロノスケットがAVプロトコルに準拠したアイソクロノスケットであることを示す。タグ907の値が1であるとき、即ち、そのアイソクロノスケットがAVプロトコル準拠のアイソクロノスケットである時には、アイソクロノスペイロード902の先頭にCIPヘッダ904が含まれる。CIPヘッダ904の中には、当該アイソクロノスケットを出力している出力装置の識別子であるソースID906が含まれる。また、CIPヘッダ904にはアイソクロノスペイロード902に含まれる実データ905がどのような種類のデータであるかをあらわすFMT908やFDF909が含まれる。映像や音声の信号は実データ905に含まれるが、実データ905はアイソクロノスペイロード902にかならず含まれるとは限らず、パケットによっては実データ905を含まずにCIPヘッダ904のみを含むアイソクロノスペイロード902も有り得る。

【0005】

また、AVプロトコル上で機器制御を行うためのコマンド群として、AV/Cコマンドセットがある。例えば、「1394 TRADE ASSOCIATION Specification for AV/C Digital Interface Command Set Version 1.0」 September 13, 1996に詳

しい。これらのコマンドとその応答はエイシンクロナス通信を用いて転送される。

【0006】

【発明が解決しようとする課題】

上記従来のデータ転送方法において、著作権保護のためにアイソクロナス通信のアイソクロノスペイロード902を暗号化して送信しようとする、暗号化されたアイソクロノスペイロード902の転送に対応していない従来の機器との互換性を保つことができない。すなわち、従来の機器はアイソクロノスペイロード902の先頭にCIPヘッダ904が正常に配置されて送信されてくることを前提に作られており、アイソクロノスペイロード902が暗号化されてCIPヘッダ904が正常に読み出せない場合には、そのアイソクロノスパケットはAVプロトコルを満たさないものとなるとともに、暗号化されたアイソクロノスパケットを受信した受信装置は正常に動作することができなくなる。すなわち実データ905に含まれる映像音声データがどのような種類のデータであるかを判別することが不可能であるとともに、当該アイソクロノスパケットを出力している装置を特定することが不可能になるので送信装置に対する各種の問い合わせ等の通信を行うことができなくなり、受信動作を正常に行うことが不可能となってしまうという課題があった。

【0007】

また、上記従来のデータ転送方法において、送信装置が出力するアイソクロノスパケットを受信装置が継続して受信している最中にアイソクロノスパケットの暗号化が始まるような場合、従来の機器においては暗号化が始まった途端にCIPヘッダ904を正常に読み出すことができなくなり、正常な受信が行えなくなるという課題があった。

【0008】

また、送信装置が、著作権で保護されている映像音声情報等を暗号化して送信し、正規に認められた受信装置が暗号化された映像音声データ等を復号化するためには、送信装置から正規の受信装置に対して復号のための鍵情報を付与する必要があるが、上記従来のデータ転送方法においては送信装置が受信装置を特定す

るには非常に煩雑な手順を実行せねばならない。すなわちアイソクロノスパケットには、送信を行っている装置の識別子であるソースID906は含まれるが、どの装置が当該アイソクロノスパケットを受信するべきであることをあらわす情報は含まれておらず、送信装置には、どの装置が当該アイソクロノスパケットの受信を行っているかを直接的に調べることはできない。そこで、送信装置において、IEEE1394バス上に接続されている機器のうちのどの機器が受信を行っており、どの機器が受信を行っていないかを調べるにはバス上の全ての機器に対して受信状態の問い合わせを行わねばならず、非常に煩雑であるという課題があった。

【0009】

本発明は上記従来の問題点を解決するもので、暗号化した映像音声情報をアイソクロノス通信で送信する場合にも従来の通信規格を満足し、かつ従来の受信装置が暗号化された映像音声データを含むアイソクロノスパケットを受信しても誤動作することのないデータ転送方法を実現することを目的とする。

【0010】

また、本発明は、送信装置が正規の受信装置に復号のための鍵情報を付与する際の手順を極めて簡素なものとするのが可能なデータ転送方法を実現することを目的とする。

【0011】

【課題を解決するための手段】

上記従来 of データ転送方法の問題点を解決するために、本発明のデータ転送方法は、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行い、データ転送を行う。

【0012】

また、本発明のデータ転送方法は、同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データと一緒に送信され、実データ部が暗号化されていることを検出した受信装置が送信装置に対して復号化情報を要求し、受信装置は送信装置から受け取った復号化情報を使用して実データ部の復号化を行うことによ

ってデータ転送が行われる。

【0013】

【発明の実施の形態】

本発明は、バス上の任意の機器が同期データを受信する同期通信と、非同期データを受信する機器が特定される非同期通信とが混在するバスシステムにおいて、前記同期データは実データ部を含む場合があり、前記実データ部の暗号化状況を示す暗号識別情報が前記実データ部以外の前記同期データ中に含まれており、前記同期データを受信した受信装置は、前記実データ部が暗号化されていることを前記暗号識別情報が示している場合には前記同期データを送信している送信装置に対して前記非同期通信を用いて前記実データ部の復号化情報を要求し、前記要求を受けた前記送信装置は前記非同期通信を用いて前記受信装置に対して前記実データの復号化情報を暗号化して送信し、前記受信装置は前記暗号化された復号化情報から前記復号化情報を取り出し、前記復号化情報を用いて暗号化された実データ部を復号する。

【0014】

これにより、以下のような作用を有する。

まず、同期データを受信した受信装置が同期データ内に含まれる暗号識別情報を調べ、実データ部が暗号化されていることを検出すると送信装置に対して実データ部を復号するための復号化情報を要求する。この要求は非同期通信を用いて行われ、この要求を受け取った送信装置においては、非同期通信のパケットヘッダを調べることにより要求を出した機器すなわち受信装置が特定される。ここで特定された受信装置に対して送信装置が復号化情報を付与することにより、送信装置が受信装置に復号のための鍵情報を付与する際の手順が極めて簡素なデータ転送方法を実現できる。

【0015】

また、同期データの暗号化は実データ部のみに対して行われ、同期データには実データ部の暗号化状況を示す暗号識別情報が含まれる。これにより、CIPヘッダは暗号化されずにそのまま転送されるので従来の装置がこれらの暗号化された同期データを受信しても誤動作することはない。すなわち、従来のデータ転送

方法との互換性を保ちつつ、かつ従来の受信装置が同期データを受信しても誤動作する可能性の無いデータ転送方法を実現できる。

【0016】

また、送信装置の送信している同期データを受信装置が継続的に受信している最中に同期データの暗号化が始まったとしても、CIPヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できる。

【0017】

以下、本発明の実施の形態について、図面を参照しながら説明する。

図1は、本発明の実施の形態において転送されるアイソクロノスケットのペイロード部の形式を表した図である。本実施の形態は、MPEGのTSP（トランスポートパケット）の伝送を例とする。暗号化情報（ENC）910は実データ905が暗号化されているか否かを示す。

【0018】

図2は、本実施の形態における送信装置と受信装置の関係をあらわすブロック図である。図2において、送信装置110と受信装置128とは1394バス111を通じてつながれている。信号源100は、1394バス111上に送信しようとする188バイト単位のMPEGのTSP（図示せず）を暗号化手段101に対して出力する。すなわち本実施の形態では、信号源100は188バイトの固定長のデータを出力する。暗号化手段101は、鍵生成手段106から与えられる暗号鍵109を用いて信号源100から入力したTSPを暗号化して出力する。本実施の形態では暗号鍵109が復号化情報に相当する。鍵生成手段106からの出力命令105は、暗号化手段101に対する命令であり、通常出力、暗号化出力、空出力の3種類の命令がある。出力命令105を入力した暗号化手段101は、その命令の内容が通常出力である場合には、信号源100から入力したTSPをそのまま出力し、暗号化情報910には値0を出力する。また出力命令105の内容が暗号化出力である場合には、TSPを、鍵生成手段106から受け取った暗号鍵109で暗号化して出力し、暗号化情報910には値1を出力する。また出力命令105の内容が空出力である場合には、信号源100から

TSPを受け取るたびに空信号（図示せず）を出力するとともに、暗号化情報910には値1を出力する。

【0019】

ソースパケット化手段102は、暗号化手段101から入力した188バイトのTSPに4バイトのソースパケットヘッダを付加して192バイトのソースパケットを出力する。CIPブロック化手段103は、ソースパケット化手段102から受け取ったソースパケットにCIPヘッダ954を付加して出力する。その際にCIPブロック化手段103は、暗号化手段101から入力した暗号化情報910をCIPヘッダ954内に配置する。アイソクロノスパケット化手段107はCIPブロック化手段103から入力したパケットにアイソクロノスパケットヘッダ900、ヘッダCRC901およびデータCRC903を付加して出力する。このとき、アイソクロノスパイロード952の内容がAVプロトコルに準拠したデータであるので、タグ907の値は1とする。鍵生成手段106は、受信装置128との間のエイシンクロナス通信のやり取りにより暗号鍵109を受信装置128に送信するとともに暗号化手段101に対しても出力する。

【0020】

1394パケット入出力手段108は1394バス111と送信装置110との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、アイソクロノスパケット化手段107の出力するアイソクロノスパケットおよび鍵生成手段106の出力するエイシンクロナスパケットを1394バス111上に出力するとともに、1394バス111から受信したエイシンクロナスパケットを鍵生成手段106へと出力する。

【0021】

1394パケット入出力手段127は、1394バス111と受信装置128との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、1394バス111から受信したアイソクロノスパケットをパイロード抽出手段123に対して出力し、1394バス111から受信したエイシンクロナスパケットを鍵生成手段125に対して出力する。また、鍵生成手段125の出力するエイシンクロナスパケットを1394バス111に対して出力す

る。

【0022】

ペイロード抽出手段123は、1394バス111から受信したアイソクロノスパケットを1394パケット入出力手段127から入力し、アイソクロノスパケットのタグ907の値が1である場合にはアイソクロノスペイロード952の中身がAVプロトコル準拠のデータであることを知り、アイソクロノスペイロード952を実データ抽出手段122に対して出力する。実データ抽出手段122は、受け取ったアイソクロノスペイロード952に実データ905が含まれる場合には、アイソクロノスペイロード952の先頭のCIPヘッダ954を除去した実データ905を復号化手段121に対して出力する。また、実データ抽出手段122は、CIPヘッダ954から抽出したソースID906と暗号化情報910とを鍵生成手段125に対して出力する。また暗号化情報910は、復号化手段121に対しても同様に出力される。鍵生成手段125は、送信装置110との間のエイシンクロナス通信のやり取りにより暗号鍵126を受け取り、復号化手段121に対して出力する。復号化手段121は、実データ抽出手段122から受信した暗号化情報910の値が0である場合には実データ抽出手段122から受け取った実データ905を映像音声化手段120に対してそのまま出力し、値が1である時には鍵生成手段125から受け取った暗号鍵126を用いて実データ905を復号化し、復号化した結果を映像音声化手段120に対して出力する。

【0023】

図3は、本実施の形態における鍵生成手段106と鍵生成手段125との間でやり取りされるAKEコマンド(AKE: Authentication and Key Exchange)のコマンドフォーマットおよびレスポンスフォーマットをあらわす図である。これらのコマンドおよびレスポンスは、AV/Cコマンドセットに属するコマンドとして、エイシンクロナス通信を用いて送信装置110と受信装置128との間でやり取りされる。これらのコマンドおよびレスポンスをやり取りすることにより、送信装置110および受信装置128の間で相手装置の認証や暗号鍵109、126のやり取りに必要な情報の交換を行う。AKEコマンドには、相手装置に対す

る何らかの動作を要求するAKEコントロールコマンドと、相手装置の状態や能力を問い合わせるためのAKEステータスコマンドとがある。

【0024】

図3(a)は、AKEステータスコマンドのフォーマットをあらわす図である。AKEステータスコマンドにおいて、オペコード208は、当該コマンドがAKEコマンドであることを示す。アルゴリズムID200は固定値0であり、0以外の値は将来の拡張のために予約となっている。

【0025】

図3(b)は、AKEステータスコマンドに対するレスポンスのフォーマットをあらわす。図3(a)のAKEステータスコマンドを受け取った装置が、AKEステータスコマンドの発行元の装置に対して返送するのがこのレスポンスである。送信装置110と受信装置128との間で相互認証および暗号鍵109, 126の伝達を行う一連の情報交換手順には複数の種類があり、アルゴリズム領域201は、当該レスポンスを返す装置が実行可能な情報交換手順の識別子がビットアサインされている。すなわち、受信装置128が、暗号化されたTSPを検出してから暗号鍵109, 126を受け取るまでの間に、送信装置110との間で複数のコマンドおよびレスポンスをやり取りする。このコマンドおよびレスポンスをやり取りする情報交換手順には複数の種類があり、当該レスポンスを返す装置はどの情報交換手順を実行可能であるかという情報がアルゴリズム領域201の各ビットによってあらわされている。アルゴリズム領域201のサイズは16ビットであるので、最大16種類の情報交換手順をあらわすことが可能である。最大データ長202は、AKEコマンドおよびそれに対するレスポンスをやり取りする際に、受信可能な最大データ長が何バイトであるかを示す。

【0026】

図3(c)は、AKEコントロールコマンドのフォーマットをあらわす。AKEコントロールコマンドにおけるアルゴリズム領域201は、アルゴリズムID200の値が0である時には、実行中の情報交換手順をあらわす。アルゴリズム領域201の各ビットは、AKEコントロールコマンドおよびAKEコントロールコマンドに対するレスポンスにおいては必ず1つのビットだけが1となってお

り、その1ビットが現在実行中の情報交換手順をあらわしている。ラベル202は、複数のAKEコントロールコマンド間の対応を明確にするために用いられる。例えば、装置が他の装置に対してAKEコントロールコマンドを送信したとして、そのAKEコントロールコマンドを受信した装置は、受信したAKEコントロールコマンドに呼応する別のAKEコントロールコマンドを返送するという規定が、ある情報交換手順で定められているとする。この場合、両AKEコントロールコマンド間の呼応関係を明確にするために、返送するAKEコントロールコマンドに挿入されるラベル202は最初に受信したAKEコントロールコマンドに挿入されていたラベル202と同じ値を使用する。ステップ番号203は、情報交換手順の中でやり取りされる個々のAKEコントロールコマンドに対して1から順に付けられるシリアル番号である。

【0027】

また、サブファンクション299は（表1）に挙げる値をとる。

【0028】

【表1】

サブファンクション	値
メイクレスポンス	00 ₁₆
ベリファイミー	01 ₁₆
クリエイトキーインフォ	10 ₁₆
リコンストラクトキー	11 ₁₆
エクスチェンジ	20 ₁₆

【0029】

サブファンクション299の内容がメイクレスポンスである場合に、当該AKEコントロールコマンドは、コマンドを受信する装置に対する認証のチャレンジを意味する。このときデータ207には、相手の装置を認証するための乱数である認証チャレンジデータが含まれる。このコマンドを受信した装置は、サブファンクション299の内容がベリファイミーであるAKEコントロールコマンドを返送する。この返送の際にデータ207に格納されるデータは、先程受信したデータ207に対してあらかじめ定められた演算を行った結果である認証レスポンス

スデータである。この演算に使用される鍵情報は、あらかじめ正規に認定された機器にのみ付与されている鍵であるので、返送されてきた認証レスポンスデータを調べれば、演算を行った機器が正しく認定された機器であるか否かを認証することができる。

【0030】

サブファンクション299の内容がクリエイトキーインフォである場合に当該AKEコントロールコマンドは、コマンドを受信する装置に対する暗号鍵109の要求を意味する。このAKEコントロールコマンドを受け取った装置は、サブファンクション299の内容がリコンストラクトキーであるAKEコントロールコマンドを返送する。この時、データ207には暗号化された暗号鍵109が格納されて返送される。

【0031】

サブファンクション299の内容がエクスチェンジである場合に当該AKEコントロールコマンドは、コマンドを送信する機器と受信する機器との間の鍵情報の交換を意味する。この鍵情報はデータ207に格納されて転送され、機器間の間接認証や、機器共有鍵の作成のために使用される。

【0032】

(表1)に挙げられている以外のサブファンクションの値は将来の拡張のための予約となっている。チャンネル番号204は、送信装置110および受信装置128の間で通信を行うアイソクロノス通信のチャンネルの番号を示す。このチャンネル番号204は、サブファンクション299の内容がクリエイトキーインフォまたはリコンストラクトキーの時にのみ有効であり、それ以外の場合にこの値は16進表記でFFとなる。ブロック番号205および総ブロック番号206は、AKEコントロールコマンドでやり取りすべきデータが一つのAKEコマンドで伝送しきれない場合に当該データを分割して送信する際に使用する。すなわち、総ブロック番号206は当該データを幾つに分割したかをあらわし、ブロック番号205によって、データ207が分割されたうちの幾つ目のデータであるかを示す。データ長209はデータ207に含まれる有効なデータのサイズをバイト数で表す。データ207はAKEコントロールコマンドによってやり取りされるデ

ータである。AKEコントロールコマンドを受信した装置はAKEコントロールコマンドに対する応答を返す。その際の応答のフォーマットおよび値は受け取ったAKEコントロールコマンドのフォーマットおよび値と同じであるが、応答にはデータ207が含まれない点だけが唯一異なる。

【0033】

図4は、送信装置110から受信装置128に対して暗号鍵109、126が送信されるまでの間に両装置間でやり取りされるAV/Cコマンドの具体例を時間軸に沿って模式的にあらわした図である。まず、図4のAV/Cコマンドのやり取りが始まるまでの両装置の動作を簡単に説明する。

【0034】

まず初期状態として、暗号化されていないTSPが送信装置110から送信されている状況を想定する。この時受信装置128は受信を行っていないものとする。信号源100から出力されるTSPが暗号化手段101に入力され、暗号化手段101は出力命令105の内容が通常出力であるのでTSPを暗号化せずにそのままソースパケット化手段102に対して出力するとともに、暗号化情報910には値0を送信する。ソースパケット化手段102は受け取ったTSPに4バイトのソースパケットヘッダを付加してCIPブロック化手段103へと出力する。CIPブロック手段103はこれに8バイトのCIPヘッダ954を付加し、アイソクロノスパケット化手段107に対してアイソクロノスペイロード952として出力する。この際、CIPヘッダ954に含まれる暗号化情報910は、暗号化手段101から入力した値である0をそのまま格納する。アイソクロノスパケット化手段107は入力したアイソクロノスペイロード952にアイソクロノスパケットヘッダ900、ヘッダCRC901およびデータCRC903を付加してアイソクロノスパケットとして1394バス111上へと出力する。この際、アイソクロノスパケットヘッダ900に含まれるタグ907の値は、当該アイソクロノスパケットがAVプロトコル準拠のアイソクロノスパケットであるので、1となる。

【0035】

信号源100から出力されるTSPが変化した時、すなわち著作権で保護され

ていない映像音声情報から著作権で保護されている映像音声情報へと切り替わった時、この変化を検出した鍵生成手段106は出力命令105を通常出力から空出力へと変化させるとともに、TSPを暗号化するための暗号鍵109を暗号化手段101に渡す。

【0036】

出力命令105の内容が空出力であるとき暗号化手段101は、信号源100からTSPを受け取るたびにソースパケット化手段102に対して空信号を出力するとともに暗号化情報910には値1が出力される。暗号化手段101から空信号を受け取ったソースパケット化手段102は、ソースパケットヘッダを付加せずに、受け取った空信号をそのままCIPブロック化手段103へと伝達する。CIPブロック化手段103は空信号を受け取ると、CIPヘッダ954だけをアイソクロノスパケット化手段107へと出力する。この時、CIPヘッダ954中の暗号化情報910は、暗号化手段101から受信した値をそのまま用いる。アイソクロノスパケット化手段107はCIPブロック化手段103から受け取ったCIPヘッダ954をアイソクロノスペイロード952としてアイソクロノスパケットを作成し、1394パケット入出力手段108へ出力する。この際、当該アイソクロノスパケットはAVプロトコルに準拠しているので、タグ907の値は1となる。1394パケット入出力手段108は受け取ったアイソクロノスパケットを1394バス111上へと出力する。当該アイソクロノスパケットは継続的に出力され、1394バス111上にはCIPヘッダ954のみをアイソクロノスペイロード952に含んだアイソクロノスパケットが継続的に流れるようになる。このアイソクロノスパケットを検出した受信装置128では、1394パケット入出力手段127がタグ907を調べ、AVプロトコルに準拠したアイソクロノスパケットであることを検出した後当該アイソクロノスパケットをペイロード抽出手段123へと出力する。ペイロード抽出手段123は受け取ったアイソクロノスパケットからアイソクロノスペイロード952を抽出して実データ抽出手段122へと出力する。実データ抽出手段122ではCIPヘッダ954に含まれる暗号化情報910とソースID906とを鍵生成手段125へと出力する。鍵生成手段125では、暗号化情報910を調べて値が1である

ことを検出したのち、ソースID906から当該アイソクロノスケットを出力しているのが送信装置110であることを知る。しかる後鍵生成手段125はAV/Cコマンドを用いて暗号鍵109、126を要求する過程、すなわち図4に示した過程へと移る。

【0037】

図4において、AKEステイタスコマンド300は受信装置128から送信装置110へと送信される。これにより受信装置128は、送信装置110が実行可能な情報交換手順を問い合わせることになる。これに応じて送信装置110はAKEレスポンス301を受信装置128に対して返送する。このAKEレスポンス301には送信装置110が実行可能な情報交換手順がアルゴリズム領域201内にビットアサインされており、受信装置128は送信装置110がどの情報交換手順を実行可能なのかを知ることができる。具体例としては、送信装置110が実行可能な情報交換手順が第2番目のものと第6番目のものの2つであった場合には、AKEレスポンス301内のアルゴリズム領域201は2進表記で「0000000000100010」となる。

【0038】

AKEレスポンス301を受信した受信装置128は、送信装置110が実行可能でかつ受信装置128自身も実行可能な情報交換手順の中から最適な1つの手順を選択し、以降その手順にしたがってAV/Cコマンドをやり取りする。いま仮に受信装置128の側で実行可能な情報交換手順が第2番目のものと第8番目のものであった場合には、送信装置110および受信装置128の双方で実行可能な情報交換手順は第2番目のものだけということになり、以降は第2番目の手順を用いて認証および情報の交換が行われることになる。この手順に含まれるAKEコントロールコマンドでは、アルゴリズムIDの値が0で、アルゴリズム領域201の値が2進表記で「0000000000000010」となる。情報交換手順で指定される手順には、各種AKEコントロールコマンドのやり取りの順番だけでなく、各AKEコントロールコマンドで送られるデータ207のフォーマットや処理方法も規定されている。

【0039】

第2番目の情報交換手順に従い、鍵生成手段125はメイクレスポンスコマンド302を送信装置110に対して送信する。このメイクレスポンスコマンド302の中のデータ207には、鍵生成手段125で発生させた2つの乱数RRaとRRbとが暗号化されて含まれているとともに、アルゴリズム領域201には第2番目の手順をあらわす識別情報が含まれている。この暗号化に際して使用する鍵は、あらかじめ正規に認められた送信装置と受信装置とに与えられている共通の秘密鍵である。メイクレスポンスコマンド302を受け取った鍵生成手段106は、受け取ったメイクレスポンスコマンド302のアルゴリズム領域201を調べて、以降は第2番目の手順を用いて認証および情報の交換を行うことを知る。鍵生成手段106は第2番目の手順を実行可能なのであるから、第2番目の手順に基づいて送信されてくるメイクレスポンスコマンド302のデータ207には秘密鍵で暗号化された2つの乱数が含まれていることを知っている。そこで鍵生成手段106は秘密鍵を用いてデータ207からRRaおよびRRbの2つの乱数を取り出したのち、レスポンスを作成することが可能であることを示す応答303を返す。しかるのち鍵生成手段106は、取り出した乱数のうちの一つであるRRaをデータ207に格納してベリファイミーコマンド304を受信装置128に対して送信する。これが先程のメイクレスポンスコマンド302にて要求されたレスポンスである。このベリファイミーコマンド304を含め、以降、送信装置110と受信装置128との間でやり取りされるAKEコマンドのアルゴリズム領域201には全て、2番目の手順をあらわす識別情報が含まれる。

【0040】

ベリファイミーコマンド304を受信した鍵生成手段125は、データ207の内容であるRRaが、自分が先程発生させた乱数RRaと相違無いことを確かめたのち、ベリファイミーコマンド304に対して正常にベリファイしたことを示す応答305を返す。これにより、鍵生成手段125は、送信装置110が正規に認められた送信装置であると認証する。

【0041】

次に送信装置110が、先程と同じメイクレスポンスコマンド306およびベリファイミーコマンド308を用いて、受信装置128が正規に認められた受信

装置であることを確認する。この際に使用される乱数はRTaおよびRTbであり、ペリファイミコマンド308で送り返される乱数はRTbである。

【0042】

この時点で送信装置110および受信装置128の双方には、乱数RRbと乱数RTbとがともにわかっていることになる。また、お互いが正規に認められた装置であることを確認したことになる。鍵生成手段106と鍵生成手段125とは、それぞれ別個に、2番目の手順で定められている共通の演算方法により、RRbとRTbとから一時鍵（図示せず）を生成する。この一時鍵は、送信装置110および受信装置128の両装置のみが共有する共通の鍵である。

【0043】

次に鍵生成手段125はクリエイトキーインフォコマンド310を送信装置110に対して送信する。この際、クリエイトキーインフォコマンド310のチャンネル番号204には、現在受信装置128が受信中のアイソクロノスパケットのチャンネル番号が格納される。このクリエイトキーインフォコマンド310を受け取った鍵生成手段106は、TSPの暗号化に用いる暗号鍵109を一時鍵で暗号化したのち、クリエイトキーインフォコマンド310が正常に完了したことを示す応答311を返送する。鍵生成手段106はTSPの暗号化に用いる暗号鍵109を一時鍵で暗号化した結果をデータ207に格納して、リコンストラクトキーコマンド312を用いて受信装置128へと送る。鍵生成手段125では一時鍵を用いてリコンストラクトキーコマンド312のデータ207を復号化し、その結果暗号鍵126を得たのち、リコンストラクトキーコマンド312を正常に完了したことをあらわす応答313を返す。暗号鍵109と暗号鍵126とは、同じ一時鍵を用いて暗号化と復号化を行ったので、同じ鍵である。暗号鍵126は鍵生成手段125から復号化手段121に対して出力される。

【0044】

リコンストラクトキーコマンド312を送信した鍵生成手段106は、暗号化手段101に対して暗号化出力を示す出力命令105を出力する。これを受けた暗号化手段101は、信号源100から受け取るTSPを暗号鍵109で暗号化し、ソースパケット化手段102への出力を開始する。これにより、1394バス111上を、暗号鍵109にて暗号化されたTSPをアイソクロノス페이ロード952に含むアイソクロノスパケットが流れるようになる。当該アイソクロノスパケットは前述したように、復号化手段121において暗号鍵126を用いて復号化され、映像音声化手段120へと出力される。

【0045】

上記一連のAKEコントロールコマンドにおいて、メイクレスポンスコマンド302とベリファイミーコマンド304、メイクレスポンスコマンド306とベリファイミーコマンド308、クリエイトキーインフォコマンド310とリコンストラクトキーコマンド312はそれぞれ同じラベル202を持つ。また、メイクレスポンスコマンド302、ベリファイミーコマンド304、メイクレスポンスコマンド306、ベリファイミーコマンド308、クリエイトキーインフォコマンド310およびリコンストラクトキーコマンド312はそれぞれ1, 2, 3, 4, 5, 6なる値をステップ番号203に持つ。

【0046】

送信装置110の出力するアイソクロノスパケットに含まれる実データ部105が、暗号化された実データ105から暗号化されない実データ105へと変化した場合には、復号化手段121は暗号化情報910の変化を検出して復号化をやめ、実データ抽出手段122から受け取った出力をそのまま映像音声化手段120へと渡すようになる。

【0047】

また、上記の図4に示した過程が始まった後に1394バス111にバスリセットが発生した場合には、メイクレスポンスコマンド302以降の手順を最初からやりなおす。

【0048】

以上のように本実施の形態によれば、アイソクロノスパケット内の実データの

暗号化状況を示す暗号化情報が実データと一緒に送信されてデータ転送が行われることにより、アイソクロノスケットを受信した受信装置がアイソクロノスケット内に含まれる暗号化情報を調べ、実データが暗号化されていることを検出すると送信装置に対して実データを復号するための暗号鍵を要求し、要求を受けた送信装置は受信装置に対して暗号鍵を付与するので、送信装置が受信装置に復号のための暗号鍵を付与する際の手順が極めて簡素なデータ転送方法を実現できる。

【0049】

また、アイソクロノス通信で転送されるアイソクロノスケットには実データの暗号化状況を示す暗号化情報と実データとが含まれ、暗号化は実データに対してのみ行ってデータ転送を行うことにより、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が暗号化された実データを受信しても誤動作する可能性のないデータ転送方法を実現できる。

【0050】

さらに、送信装置の送信している同期データを受信装置が継続的に受信している最中に同期データの暗号化が始まったとしても、CIPヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できる。

【0051】

なお、本実施の形態においては、暗号鍵による暗号化が一旦開始すれば全ての転送単位に含まれる実データは暗号化されて送信されるが、全ての転送単位に対して暗号化を行う必要はない。例えば、暗号化された転送単位と暗号化されない転送単位とが交互に送信されても、CIPヘッダ中に暗号化情報が含まれているので受信装置においては復号を正常に行うことが可能であり、同様の効果を得ることが可能である。この場合、暗号化を行う転送単位の割合を受信装置が送信装置に指定しても得られる効果が変わらないことは言うまでもない。また、MPEGのソースパケットはその大きさが192バイトであるが、MPEGの高データレート転送(12Mbps以上)を行う際には複数のソースパケットが一つのアイソクロノスペイロードに格納される。このとき、同一のアイソクロノスペイロ

ードの中に、暗号化されたソースパケットと暗号化されないソースパケットとの両方があってはならないことも言うまでもない。

【0052】

また、本実施の形態においては、暗号鍵による暗号化は実データ部全てに対して行われたが、全ての部分に暗号化を行う必要はない。例えば実データ部の前半分だけを暗号化したり、実データ部を4等分したうちの最初と3番目の2個所を暗号化して送信しても同様の効果が得られる。この場合は暗号化を行った場所や割合を示す情報をCIPヘッダに挿入して送信すれば受信装置側で適切な復号化を行うことが可能である。また、CIPヘッダには実データが暗号化されているか否かを示す暗号化情報のみを挿入しておき、CIPヘッダを見て暗号化されていることを検出した受信装置が、どの部分がどのくらい暗号化されているかという情報をエイシンクロナス通信を用いて送信装置に問い合わせても同様の効果を得ることが可能である。この場合、暗号化を行う場所や割合を受信装置の側が送信装置に対してエイシンクロナス通信を用いて指定しても同様の効果が得られることは言うまでもない。また、実データ部の中でデータの重要性が高い部分についてのみ暗号化を行うと、暗号化および復号化にかかる負荷が低いにもかかわらず十分な暗号化の効果が得られることも言うまでもない。

【0053】

また、本実施の形態においては、送信装置と受信装置との間の相互の認証が完了するまでの間は実データを含まないCIPヘッダのみのアイソクロノスパケットを転送したが、CIPヘッダのみのアイソクロノスパケットを出力することなく最初から暗号化された実データを含むアイソクロノスパケットを出力しても同様の効果が得られることは言うまでもない。

【0054】

また、本実施の形態においては、送信装置と受信装置の間でやり取りされるAKEコントロールコマンドの転送手順を相互の調停により決定したが、受信装置が実行可能な手順が一つだけに限られる場合にはこの調停手順を行わず、受信装置が実行可能な唯一の手順でコマンドの転送を開始しても同様の効果が得られることは言うまでもない。こういった場合には、全ての正規に認証された機器が最

低限実行可能な基本手順を定めておくことが望ましい。

【0055】

また、本実施の形態においては、送信装置と受信装置との間で直接認証を行い、秘密鍵による復号化情報の伝送を行ったが、認証および復号化情報の伝達手段はこれに限らない。例えば公開鍵を用いて相互に間接認証および一時鍵の作成を行い、一時鍵を用いて復号化情報の伝送を行っても構わない。以下、その手順を簡単に説明する。

【0056】

送信装置および受信装置は、相互の調停の結果定められた手順により、相互の間接認証に必要となる鍵情報をAKEコントロールコマンドのデータ207に格納して送信しあう。このとき、サブファンクション299はエクスチェンジをあらわす。これにより、送信装置と受信装置は互いに正規に認証された機器であれば同じ一時鍵を共有することになるので、それ以降は本実施の形態と同様にクリエイトキーインフォコマンドおよびリコンストラクトキーコマンドを用いて復号化情報の伝送を行うことが可能となる。

【0057】

【発明の効果】

以上のように本発明のデータ転送方法では、同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データ部と一緒に送信されてデータ転送が行われることにより、同期データを受信した受信装置が同期データ内に含まれる暗号識別情報を調べ、実データ部が暗号化されていることを検出すると送信装置に対して実データ部を復号するための復号化情報を要求し、要求を受けた送信装置は受信装置に対して復号化情報を付与するので、送信装置が受信装置に復号のための鍵情報を付与する際の手順が極めて簡素なデータ転送方法を実現できるという優れた効果がある。

【0058】

また、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行ってデータ転送を行うことにより、従来のデータ転送方法との互換性を保ちつつ、かつ

従来の受信装置が暗号化された同期データを受信しても誤動作する可能性の無いデータ転送方法を実現できるという優れた効果がある。

【0059】

また、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行ってデータ転送を行うことにより、送信装置の送信している同期データを受信装置が継続的に受信している最中に同期データの暗号化が始まったとしても、CIPヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できるという優れた効果がある。

【0060】

また、送信装置と受信装置の間でやり取りされる認証情報および復号化情報の授受手順を送信装置と受信装置との間の調停によって選択することにより、将来の拡張性に優れた認証および復号化情報の授受手順を実現することが可能となる。すなわち、将来新しい認証方法や復号化情報が利用可能になった際に、新しい手順を使用できる機器と古い手順しか使用できない機器とが混在しても、新しい機器側で古い手順を使用可能であれば、両機器間の調停により最適な手順を選択することが可能になる。すなわち本発明のデータ転送方法では、新しい機器と古い機器とが混在する環境においても、常に最適な手順を選択して実行可能になるという優れた効果がある。

【0061】

また、暗号化された実データと暗号化されない実データとの割合を変化させることが可能であるので、暗号化された実データを復号するための特別なハードウェアを持たない受信装置でもソフトウェアによって復号化が可能になる。すなわち、パソコンのように特別な復号のためのハードウェアを持たない機器が受信装置である場合にも、暗号化される実データの割合を低下させることによりソフトウェアによる復号が可能になるという優れた効果がある。

【0062】

また、実データの中で暗号化する部分や割合を変化させることが可能であるので、暗号化された実データを復号するための特別なハードウェアを持たない受信

装置でもソフトウェアによって復号化が可能になる。すなわち、パソコンのように特別な復号のためのハードウェアを持たない機器が受信装置である場合にも、実データの中で暗号化する部分の割合を低下させることによりソフトウェアによる復号が可能になるという優れた効果がある。

【0063】

また、送信装置と受信装置が相互に正規の機器であることを認証するまでの間は実データを含まないアイソクロノスケットを出力するので、限られたバスの転送帯域を無駄に使用することがなく、また正規に認証されていない機器が実データを受信してしまう可能性が非常に少なくなるという優れた効果がある。

【図面の簡単な説明】

【図1】

本発明の実施の形態におけるCIPヘッダのフォーマットを表す模式図

【図2】

同実施の形態における送信装置と受信装置との構成を示すブロック図

【図3】

(a) 同実施の形態におけるAKEステータスコマンドのフォーマットを表す説明図

(b) 同実施の形態におけるAKEステータスコマンドに対するAKEレスポンスのフォーマットを表す説明図

(c) 同実施の形態におけるAKEコントロールコマンドのフォーマットを表す説明図

【図4】

同実施の形態による送信装置と受信装置との間のエイシンクロナスケットの授受を表す模式図

【図5】

従来のデータ転送方法におけるアイソクロノスケットのフォーマットを表す説明図

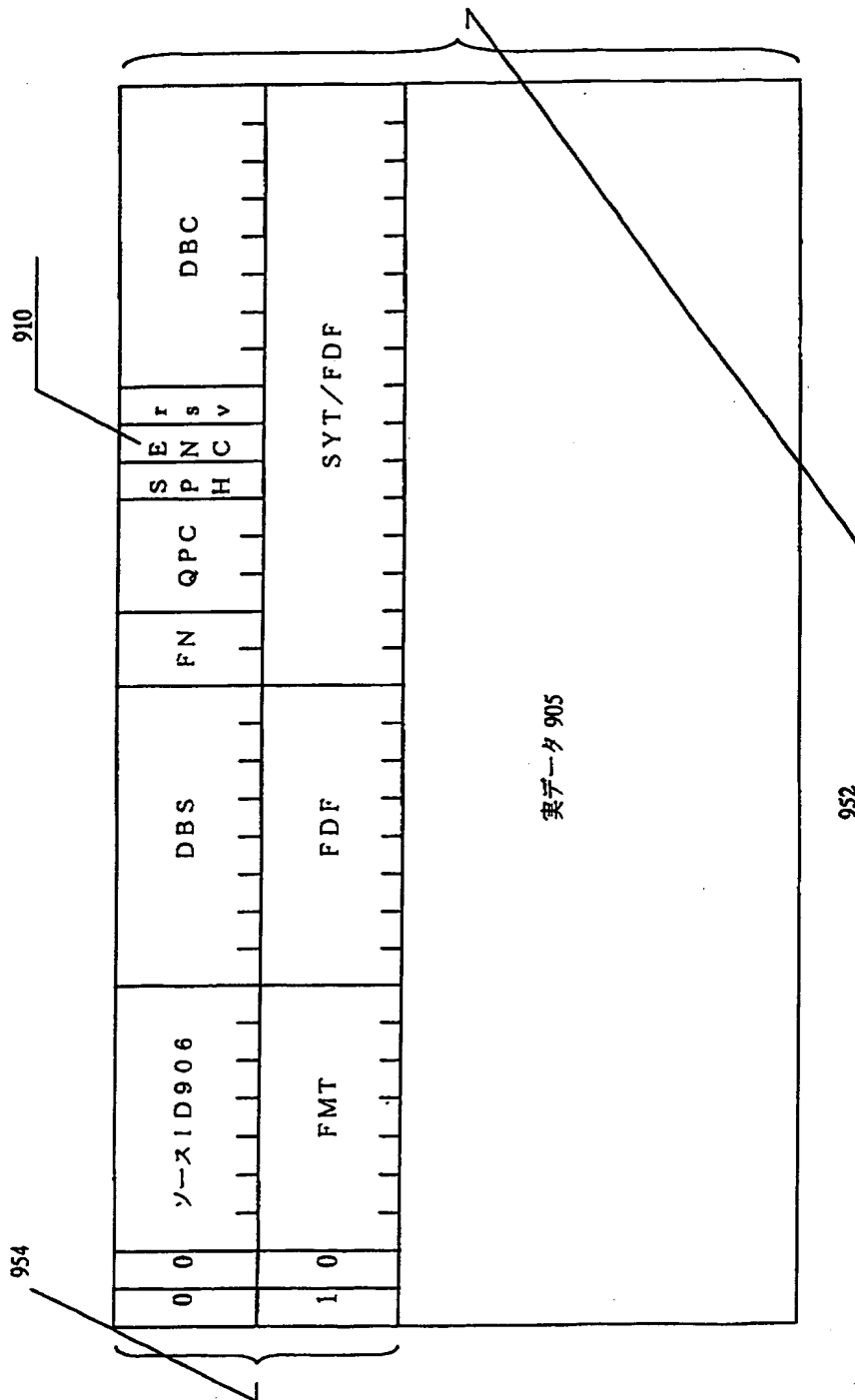
【符号の説明】

101 暗号化手段

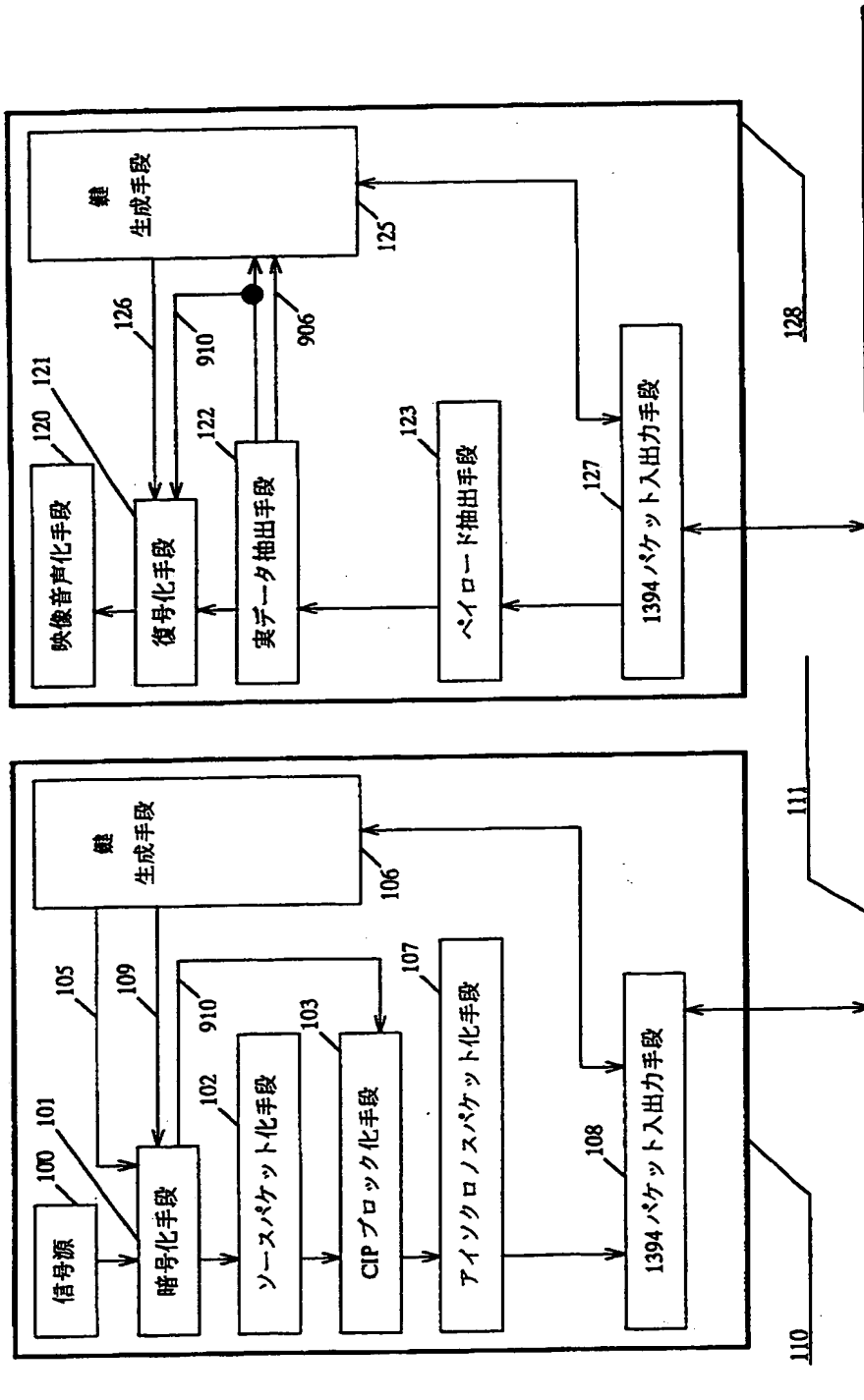
- 102 ソースパケット化手段
- 103 CIPブロック化手段
- 106、125 鍵生成手段
- 107 アイソクロノスパケット化手段
- 108、127 1394パケット入出力手段
- 110 送信装置
- 111 IEEE1394バス
- 121 復号化手段
- 122 実データ抽出手段
- 123 ペイロード抽出手段
- 128 受信装置
- 900 アイソクロノスパケットヘッダ
- 901 ヘッダCRC
- 902、952 アイソクロノスペイロード
- 903 データCRC
- 904、954 CIPヘッダ
- 905 実データ
- 906 ソースID
- 907 タグ
- 910 暗号化情報

【書類名】 図面

【図 1】



【図2】



【図3】

(a)

		オペコード 208							
msb								lsb	
opcode		Authentication and Key exchange							
operand[0]		F ₁₆				アルゴリズム I D200			
operand[1]		FF ₁₆							
operand[2]		FF ₁₆							
operand[3]		FF ₁₆							
operand[4]		FF ₁₆							
operand[5]		FF ₁₆							
operand[6]		FF ₁₆							
operand[7]		FF ₁₆							
operand[8]		FF ₁₆							

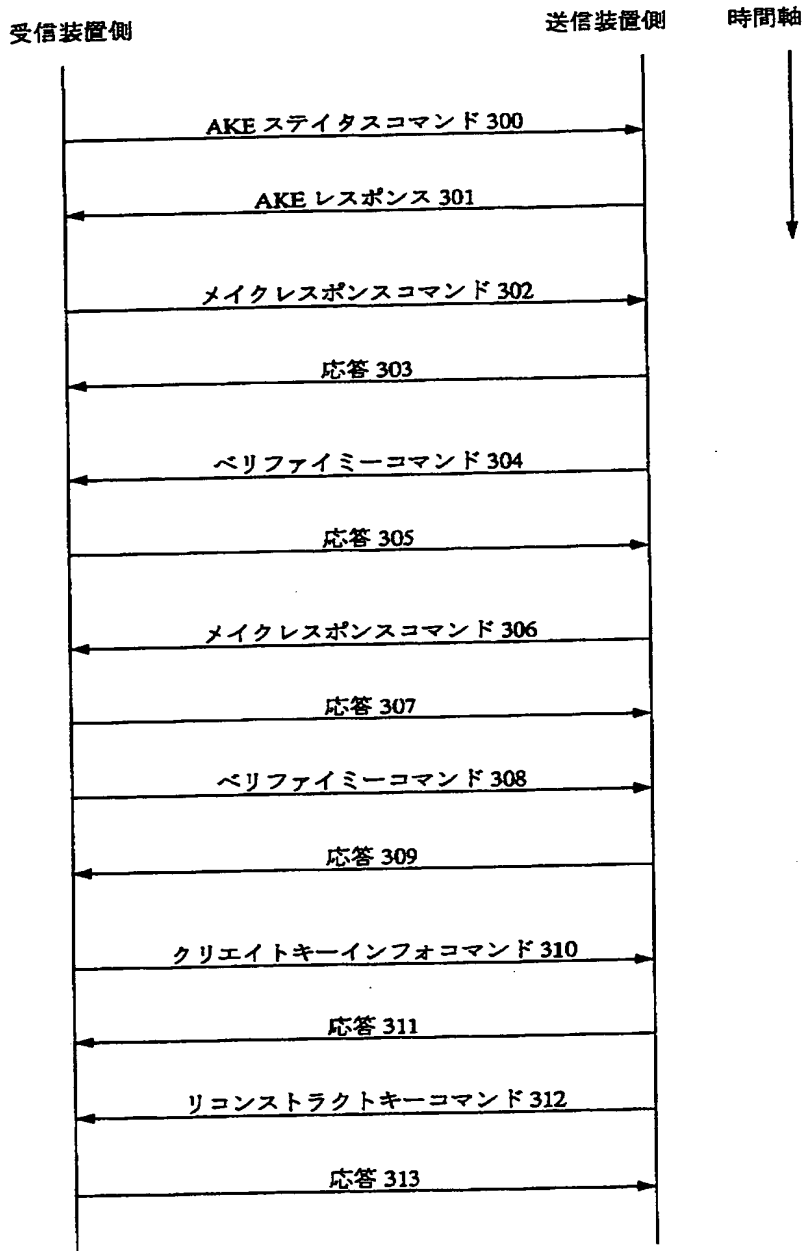
(b)

	msb	オペコード 208				lsb
opcode	Authentication and Key exchange					
operand[0]	0			アルゴリズム I D200		
operand[1]	(msb)	アルゴリズム領域201				(lsb)
operand[2]						
operand[3]	FF ₁₆					
operand[4]	FF ₁₆					
operand[5]	FF ₁₆					
operand[6]	FF ₁₆					
operand[7]	(msb)	最大データ長202				(lsb)
operand[8]						

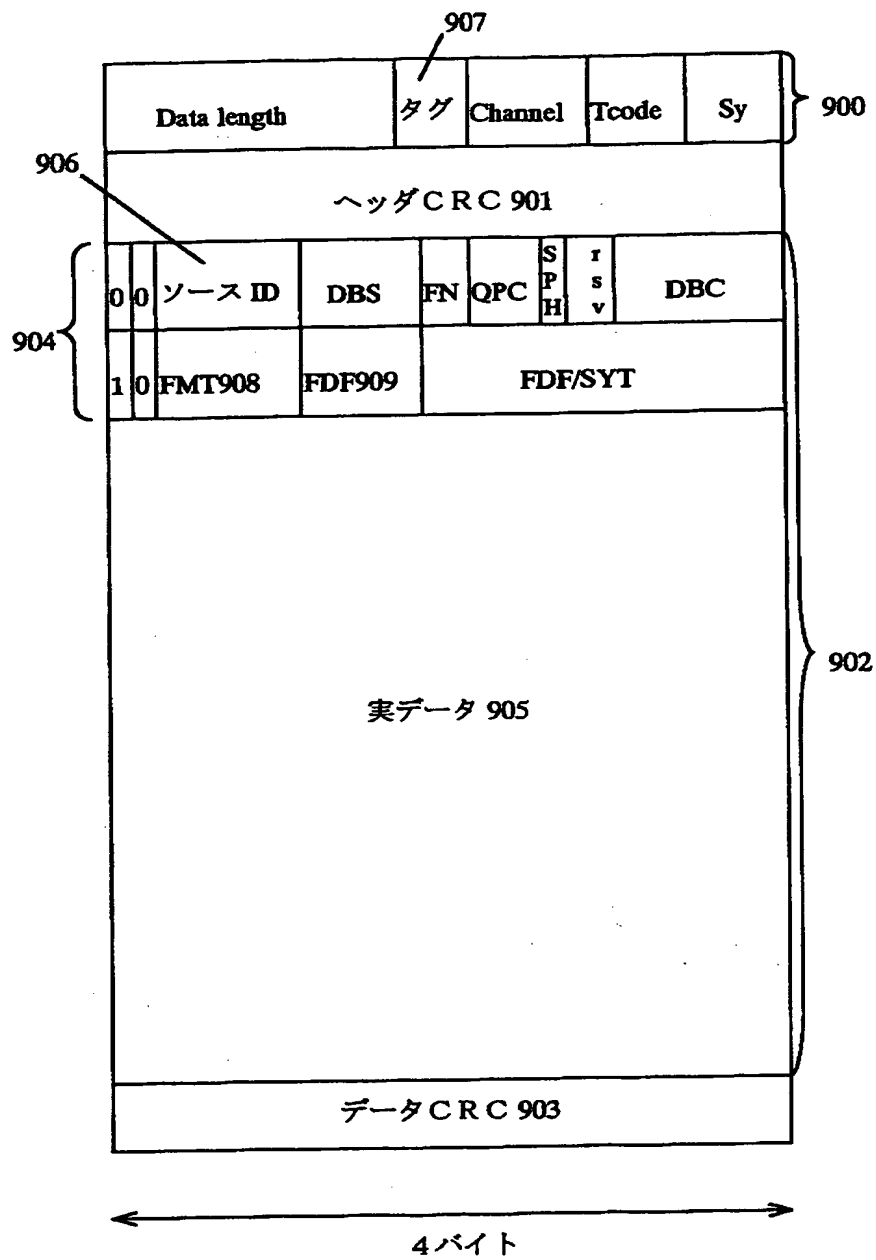
(c)

		オペコード 208				lsb	
msb							
opcode		Authentication and Key exchange					
operand[0]		reserved			アルゴリズム I D200		
operand[1]		(msb) アルゴリズム領域201					(lsb)
operand[2]							
operand[3]		ラベル202			ステップ番号203		
operand[4]		サブファンクション299					
operand[5]		チャンネル番号204					
operand[6]		ブロック番号205			総ブロック番号 206		
operand[7]		(msb) データ長209					(lsb)
operand[8]							
operand[9]		データ207					
:							
operand[8+data_length]							

【図4】



【図5】



【書類名】 要約書

【要約】

【課題】 IEEE1394バスで、著作権により保護されたAV情報を暗号化して送信する際に、暗号化に対応していない従来の機器も誤動作することのないデータ転送方法を提供することを目的とする。

【解決手段】 暗号化は実データ部905に対してのみ行い、ヘッダ954は暗号化せずに送信する。実データ部905が暗号化されているかどうかを示す暗号識別情報910がヘッダ954内に配置される。これにより、従来の規格を満し、かつ従来の機器が暗号化されたパケットを受信しても誤作動することがない。

【選択図】 図1

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000005821

【住所又は居所】 大阪府門真市大字門真1006番地

【氏名又は名称】 松下電器産業株式会社

【代理人】 申請人

【識別番号】 100078204

【住所又は居所】 大阪府門真市大字門真1006 松下電器産業株式
会社内

【氏名又は名称】 滝本 智之

【選任した代理人】

【識別番号】 100097445

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業
株式会社内

【氏名又は名称】 岩橋 文雄

特平 9-106995

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社